Avaliação de Frameworks de Gestão de Risco Cibernético

Matheus de Andrade, Ferrucio de Franco Rosa,
Amândio Ferreira Balcão Filho
UNIFACCAMP
Campo Limpo Paulista, SP, Brasil

Resumo

Frameworks de gestão de risco cibernético oferecem diretrizes estruturadas que auxiliam as organizações na identificação, avaliação e mitigação de ameaças cibernéticas. Esses frameworks variam em termos de abrangência, aplicabilidade e custo, tornando a escolha do framework certo uma decisão crítica que deve ser adaptada às necessidades específicas de cada organização. A pesquisa proposta tem como objetivo desenvolver uma abordagem para avaliar e comparar os diversos frameworks de gestão de risco cibernético, sejam eles gratuitos ou pagos, amplamente adotados ou voltados para setores específicos. A avaliação deverá considerar critérios como abrangência, adaptabilidade, eficácia, custo e conformidade regulatória.

1 Introdução

As ameaças cibernéticas evoluem em complexidade e sofisticação, colocando em risco operações críticas e informações sensíveis em organizações de todos os tamanhos [1]. Ataques como ransomware, phishing, e intrusões em sistemas destacam a necessidade urgente de uma gestão de riscos cibernéticos eficaz. A pandemia de COVID-19 acelerou essa necessidade, expandindo as superfícies de ataque com o aumento do trabalho remoto e a dependência de tecnologias digitais.

Para enfrentar esses desafios, frameworks de gestão de risco cibernético oferecem diretrizes estruturadas que auxiliam as organizações na identificação, avaliação e mitigação de ameaças cibernéticas [2]. Esses frameworks variam em termos de abrangência, aplicabilidade e custo, tornando a escolha do framework certo uma decisão crítica que deve ser adaptada às necessidades específicas de cada organização [3].

A pesquisa proposta tem como objetivo desenvolver uma abordagem para avaliar e comparar os diversos frameworks de gestão de risco cibernético, sejam eles gratuitos ou pagos, amplamente adotados ou voltados para setores específicos. Como exemplos de frameworks, podemos citar o NIST Cybersecurity Framework, de aplicaçãp geral, e o C2M2, voltado aos setores de energia e gás natural. A avaliação deverá considerar critérios como abrangência, adaptabilidade, eficácia, custo, conformidade regulatória e a integração do fator humano, essencial para a implementação eficaz das práticas de segurança.

2 Síntese da Abordagem Proposta

A abordagem de avaliação está sendo desenvolvida a partir de uma análise crítica dos frameworks existentes, complementada por uma revisão abrangente da literatura. Para garantir uma avaliação completa e imparcial, estão sendo definidos 12 critérios específicos que abrangem aspectos essenciais para a eficácia de um framework. Como exemplos de critérios de avaliação podemos citar os seguintes:

Custo: Avalia os custos de implementação e manutenção do framework, abrangendo aspectos (subcritérios) como implementação, licenciamento, treinamento, manutenção e consultoria.

Segurança da Informação: Mede a efetividade do framework na proteção de informações críticas, com foco na proteção de dados, detecção de intrusões, resposta a incidentes, recuperação e prevenção.

Eficiência: Avalia a capacidade do framework em otimizar processos e recursos de segurança, considerando a otimização de recursos, tempo de resposta, automatização, escalabilidade e integração.

Cada framework receberá uma pontuação de 1 a 5 (escala Likert) para cada subcritério, onde 1 representa a menor eficácia ou maior dificuldade, e 5 representa a maior eficácia ou menor dificuldade. A nota final de cada avaliação do framework será calculada usando as Equações 1 e 2. O processo de cálculo está sendo trabalhado para aceitar n avaliações de n frameworks, de modo a permitir a geração de rankings considerando os 12 critérios definidos.

$$N(C_i) = \frac{\sum_{j=1}^{n} (N(S_{ij}) \times P(S_{ij}))}{\sum_{j=1}^{n} P(S_{ij})} \tag{1}$$

onde $N(S_{ij})$ é a nota atribuída ao subcritério S_{ij}, e $P(S_{ij})$ é o peso do subcritério S_{ij}.

A nota final (NF) da avaliação do framework é calculada como segue:

$$NF = \frac{\sum_{i=1}^{m} (N(C_i) \times P(C_i))}{\sum_{i=1}^{m} P(C_i)} \tag{2}$$

onde $N(C_i)$ é a nota ponderada do critério C_i, e $P(C_i)$ é o peso do critério C_i.

3 Resultados Preliminares

No estágio atual da pesquisa, simulações estão sendo conduzidas para exercitar e ajustar as equações e as questões a serem propostas em cada item das escalas dos critérios e subcritérios. As simulações incluem analisar diferentes frameworks e cenários organizacionais, variando em termos de tamanho, setor de atuação e recursos disponíveis.

A análise preliminar sugere que a adaptabilidade dos frameworks varia significativamente de acordo com o contexto em que são aplicados. Por exemplo, frameworks como o NIST Cybersecurity Framework e os CIS Controls têm mostrado uma flexibilidade promissora para pequenas e médias empresas, enquanto frameworks mais complexos, como o C2M2, requerem uma maior maturidade organizacional.

Além disso, estamos avaliando o impacto dos custos de implementação e manutenção dos frameworks, considerando tanto os custos diretos quanto indiretos. Os resultados iniciais indicam que, embora alguns frameworks possam parecer mais acessíveis inicialmente, os custos associados à sua implementação completa e à formação contínua dos

funcionários podem representar desafios significativos para organizações com recursos limitados.

Conforme avançarmos nos testes e coletarmos mais dados, esperamos refinar essas análises e fornecer resultados mais conclusivos. A próxima etapa envolve a validação dos resultados em estudos de casos reais, que fornecerão uma base mais sólida para comparar a eficácia prática dos frameworks em diferentes contextos.

Em termos de produção científica, uma revisão sistemática da literatura foi conduzida e está sob revisão para posterior submissão a uma conferência internacional.

4 Conclusão

O desenvolvimento de métricas padronizadas para a avaliação contínua de frameworks é essencial para garantir que as práticas de segurança cibernética permaneçam eficazes e adaptáveis frente a um cenário de ameaças em constante mudança.

Este estudo apresentou a síntese de uma abordagem para avaliar e comparar frameworks de gestão de risco cibernético. Resultados preliminares indicam que os frameworks são complementares e mais adequados a certos contextos e domínios.

Espera-se que a abordagem proposta seja uma ferramenta importante durante o processo de escolha do framework mais adequado às necessidades específicas das organizações, considerando fatores críticos, como custo, escalabilidade, conformidade e a integração do fator humano na segurança cibernética.

References

[1] S. Purkait and M. Damle, "Cyber security and frameworks: A study of cyber attacks and methods of prevention of cyber attacks," in *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 2023, pp. 1310–1315.

[2] A. Palia, C. Devlin, M. Yelorda, and A. Morrison, "Program controls effectiveness measurement framework metrics," in *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, 2021, pp. 369–373.

[3] O. Giuca, T. M. Popescu, A. M. Popescu, G. Prostean, and D. E. Popescu, "A survey of cybersecurity risk management frameworks," in *Soft Computing Applications*, V. E. Balas, L. C. Jain, M. M. Balas, and S. N. Shahbazova, Eds. Cham: Springer International Publishing, 2021, pp. 240–272.